

Weight Distributions of Hamming Codes (II)

Dae San Kim, *Member, IEEE*

Abstract—In a previous paper, we derived a recursive formula determining the weight distributions of the $[n = (q^m - 1)/(q - 1), n - m, 3]$ Hamming code $H(m, q)$, when $(m, q - 1) = 1$. Here q is a prime power. We note here that the formula actually holds for any positive integer m and any prime power q , without the restriction $(m, q - 1) = 1$.

Index Terms—Hamming code, weight distribution, Pless power moment identity.

I. INTRODUCTION

The q -ary Hamming code $H(m, q)$ is an $[n = (q^m - 1)/(q - 1), n - m, 3]$ code which is a single-error-correcting perfect code. From now on, q will indicate a prime power unless otherwise stated. Also, assume that $m > 1$.

Moisio discovered a handful of new power moments of Kloosterman sums over \mathbb{F}_q , when the characteristic of \mathbb{F}_q is 2 and 3 ([3], [4], [6], [7]). The idea is, via Pless power moment identity, to connect moments of Kloosterman sums and frequencies of weights in the binary Zetterberg code of length $q + 1$, or those in the ternary Melas code of length $q - 1$.

In [1], we adopted his idea of utilizing Pless power moment identity and exponential sum techniques so that we were able to derive Theorem 1 below under the restriction that $(m, q - 1) = 1$. This restriction was needed to assume that $H(m, q)$ is cyclic (cf. Theorem 3). It is somewhat surprising that there has been no such recursive formulas giving the weight distributions of the Hamming codes in the nonbinary cases, whereas there has been one in the binary case (cf. Theorem 2).

In this correspondence, we will give an elementary proof showing that the restriction $(m, q - 1) = 1$ can be removed.

Theorem 1: Let $\{C_h\}_{h=0}^n$ ($n = (q^m - 1)/(q - 1)$) denote the weight distribution of the q -ary Hamming code $H(m, q)$. Then, for h with $1 \leq h \leq n$,

$$h!C_h = (-1)^h q^{m(h-1)} (q^m - 1) + \sum_{i=0}^{h-1} (-1)^{h+i+1} C_i \sum_{t=i}^h t! S(h, t) q^{h-t} (q - 1)^{t-i} \binom{n-i}{n-t}, \quad (1)$$

where $S(h, t)$ denotes the Stirling number of the second kind defined by

$$S(h, t) = \frac{1}{t!} \sum_{j=0}^t (-1)^{t-j} \binom{t}{j} j^h. \quad (2)$$

Theorem 2 (*p.129 in [2]*): Let $\{C_h\}_{h=0}^n$ ($n = (2^m - 1)$) denote the weight distribution of the binary Hamming code

$H(m, 2)$. Then the weight distribution satisfies the following recurrence relation:

$$C_0 = 1, \quad C_1 = 0,$$

$$(i + 1)C_{i+1} + C_i + (n - i + 1)C_{i-1} = \binom{n}{i} \quad (i \geq 1).$$

Theorem 3 ([5]): Let $n = (q^m - 1)/(q - 1)$, where $(m, q - 1) = 1$. Let γ be a primitive element of \mathbb{F}_{q^m} . Then the cyclic code of length n with the defining zero γ^{q-1} is equivalent to the q -ary Hamming code $H(m, q)$.

II. PROOF OF THEOREM 1

We know that the formula (1) holds for $(m, q - 1) = 1$ ([1, Theorem 1]). By the recursive formula in (1), we see that all C_i ($i = 0, 1, 2, \dots, n = (q^m - 1)/(q - 1)$) are formally polynomials in q with rational coefficients, which depend on m (cf. Corollary 2 in [1] for the explicit expressions of C_i for $i \leq 10$). Put $C_i = P_i(q; m)$, for $i = 0, 1, 2, \dots, n = (q^m - 1)/(q - 1)$. Then (1) can be rewritten as

$$h!P_h(q; m) = (-1)^h q^{m(h-1)} (q^m - 1) + \sum_{i=0}^{h-1} (-1)^{h+i+1} P_i(q; m) \sum_{t=i}^h t! S(h, t) q^{h-t} (q - 1)^{t-i} \binom{\frac{q^m-1}{q-1}-i}{t-i}, \quad (3)$$

($1 \leq h \leq n = (q^m - 1)/(q - 1)$).

Let m, h be fixed positive integers. Then the LHS and the RHS of (3) are formally polynomials in q and (3) is valid whenever q is replaced by prime powers p^r satisfying $(m, p^r - 1) = 1$ and $h \leq (p^{rm} - 1)/(p^r - 1)$.

So it is enough to show that there are infinitely many prime powers p^r such that $(m, p^r - 1) = 1$, since then (3) is really a polynomial identity in q , so that the restriction of our concern can be removed. There are three cases to be considered.

Case 1) 2 does not divide m .

Let $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where p_1, p_2, \dots, p_r are distinct odd primes and e_j 's are positive integers. Then, by Dirichlet's theorem on arithmetic progressions, there are infinitely many prime numbers p such that $p \equiv 2 \pmod{m}$. For each such an p , $p \equiv 2 \pmod{p_j}$, for $j = 1, \dots, r$. Then p_j does not divide $p - 1$, for all j , so that all p_j is relatively prime to $p - 1$. So $(m, p - 1) = 1$, for all such primes p .

Case 2) 2 is the only prime divisor of m .

In this case, $2^l - 1$ ($l = 1, 2, \dots$) are all relatively prime to m .

Case 3) 2 and some odd prime divide m .

Let $m = 2^e m_1$, $m_1 = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where e, e_1, \dots, e_r, r are positive integers and p_1, p_2, \dots, p_r are distinct odd primes. Noting that $(2, m_1) = 1$, we let $f = \text{ord}_{m_1} 2$ be the order of 2 modulo m_1 . Then $2^{lf} \equiv 1 \pmod{m_1}$, for all positive integers l . So $2^{lf} \equiv 1 \pmod{p_j}$, for all $j = 1, \dots, r$. Thus $2^{lf+1} \equiv 2 \pmod{p_j}$, for all j , and hence p_j does not divide

$2^{lf+1} - 1$, for all j . This implies that $(m, 2^{lf+1} - 1) = 1$, for all positive integers l . ■

REFERENCES

- [1] D. S. Kim, "Weight distributions of Hamming codes," submitted.
- [2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands : North-Holland, 1998.
- [3] M. Moisio, "The moments of a Kloosterman sum and the weight distribution of a Zetterberg type binary cyclic code," *IEEE Trans. Inf. Theory*, vol. IT-53, pp. 843-847, 2007.
- [4] M. Moisio, "On the moments of Kloosterman sums and fibre products of Kloosterman curves," *Finite Fields Appl.*, in Press.
- [5] V. S. Pless, W. C. Huffman, and R. A. Brualdi, "An introduction to algebraic codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands : North-Holland, 1998, vol. I, pp. 3-139.
- [6] R. Schoof and M. van der Vlugt, "Hecke operators and the weight distribution of certain codes," *J. Combin. Theory Ser. A*, vol. 57, pp. 163-186, 1991.
- [7] G. van der Geer, R. Schoof and M. van der Vlugt, "Weight formulas for ternary Melas codes," *Math. Comp.*, vol 58, pp. 781-792, 1992.